

REMARKS

This paper is in response to the Office Action dated July 30, 2007. Applicant has amended the application as set forth above. Specifically, Claims 1, 3, 4, 6-10 have been amended, and Claims 2 and 5 have been canceled without prejudice. Upon the entry of the amendments, Claims 1, 3, 4, 6-10 are pending in this application. Applicant respectfully requests the entry of the amendments and reconsideration of the application in view of the above amendments and the following remarks.

Discussion of Objection to Claims 1-10

The Examiner objected Claims 1-10 because of the informalities. In response, Applicant has amended Claims 1, 3, 4, 6-10 and canceled Claims 2 and 5 as indicated above. Withdrawal of the objection to the claims is respectfully requested.

Discussion of Rejections Under 35 U.S.C. §103(a)

The Examiner rejected Claims 1-10 under 35 U.S.C. § 103 (a) as being unpatentable over Cheng et al. (US Patent # 7107609 B1) in view of Fontes et al. (US Patent # 7058718 B2). Applicant has amended the claims and respectfully disagrees with the Examiner, and submits that the amended Claims 1, 3, 4, 6-10 are patentable over the cited references.

Disclosure of Cheng

Cheng discloses a stateful packet forwarding in a firewall cluster, in which the receiving device sends a multicast to all other firewall devices in the firewall cluster and the home device receives the multicast and responds, indicating that it is the home device. (See, e.g., Abstract and FIG. 2.)

Claim 1

As Claim 1 recites (emphasis added):

A method of sharing a state between stateful firewalls on a multiple entry/exit point (MEP) network for data exchange between a server and a client through firewalls physically remote from each other, comprising the steps of:

(a) one of the firewalls receiving an SYN packet sent from the client to the server, wherein the firewalls share a synchronized time counter, which is increased at regular intervals, and a same secret key, wherein the SYN packet comprises an Initial Sequence Number (ISN);

(b) the firewall creating a modified SYN cookie (hereinafter referred to as an m.SYN cookie), modifying the SYN packet using the m.SYN cookie and sending the SYN packet to the server, and the server sending a SYN/ACK packet to the client in response to the SYN packet, wherein the m.SYN cookie comprises upper bits of the ISN of the SYN packet, bits of time indicated by the time counter of the firewall, which creates the m.SYN cookie, at a time of creation of the m.SYN cookie, bits of an output value of a hash function, and at least some bits of the time indicated by the time counter of the firewall, wherein the hash function comprises variables for a secret key, a source address, a source port number, a destination address, a destination port number, at least some partial bits of the ISN, a time indicated by the time counter of the firewall, which creates the m.SYN cookie, at the time of creation of the m.SYN cookie;

(c) the firewall, which has received the SYN/ACK packet, extracting a firewall identifier ID_{fw} from the SYN/ACK packet and sending the SYN/ACK packet to a corresponding one of the firewalls, the corresponding firewall searching a state table for connection information and sending the connection information, together with the SYN/ACK packet, to the firewall, which has received the SYN/ACK packet; and

(d) the firewall, which has re-received the SYN/ACK packet, updating the state table, changing an acknowledgement number of the SYN/ACK packet to an Initial Sequence Number (ISN_c)+1, and sending the SYN/ACK packet to the client.

Cheng Does Not Teach or Suggest Claims 1-10

As the Examiner correctly pointed out, Cheng does not disclose a modified SYN cookie that will allow for a modification of a SYN packet and SYN/ACK.

In addition to the lack of m.SYN cookie, the modified SYN cookie, Cheng does not teach or suggest another feature of the present invention.

In lines 12-19, page 3 of the July 30, 2007 Office Action, the Examiner stated that “The receiving device (i.e. a firewall) will send out a signal and the first data packet from the data 120-packet flow to all firewalls on the firewall cluster to see who is the home device or the requesting host device. All firewalls will update their state table and forwarding tables; once the home

device or requesting device is found the, the firewall that didn't request the data 120 from the internet will update its state table and forwarding table and forward all data 120 packets to the home device and host respectively. Col 4, lines 38-67 & Col 5, lines 1-3; Col. 4, lines 4-10."

As the Examiner pointed out correctly above, the receiving devices (i.e. a firewall) has to send out the signal and the first data packet to all firewalls on the firewall cluster to see who is the home device or the requesting host device. That is, the device "B" sends multicast request with data packet and device information. (See, e.g., also Fig. 2.)

In contrast, the SYN/ACK packet does not have to be sent to all firewalls, but "sending the SYN/ACK packet to a corresponding one of the firewalls" is enough in the present invention. (See, e.g., the underlined portion of Claim 1.) In the present invention, as shown in Fig. 6, the right client can be zeroed in without multicasting the information to all firewalls.

As such, Cheng does not disclose every features of Applicant's Claims 1-10, and therefore does not anticipate Claims 1-10.

Accordingly, Applicant respectfully requests that the 103(a) rejection of Claims 1-10 be withdrawn.

Disclosure of Fontes

Fontes discloses a method of producing a blended SYN cookie, which includes identifying within a SYN packet a source network address and desired communications session parameters. Fontes's method is for combating DoS flood and quasi-TCP attacks using a three-way handshake method which utilizes the blended SYN cookies.

Cheng and Fontes Do Not Teach or Suggest Claims 1-10

As the Examiner pointed out, Fontes discloses a blended SYN cookie.

First, however, the blended SYN cookie still does not remedy the deficiencies of Cheng as shown in the above.

Second, the m.SYN cookie of the present invention is distinctly different from the blended SYN cookie disclosed by Fontes.

As emphasized in the amended Claim 1 in the above, "the m.SYN cookie comprises upper bits of the ISN of the SYN packet, bits of time indicated by the time counter of the firewall, which creates the m.SYN cookie, at a time of creation of the m.SYN cookie, bits of an output

value of a hash function, and at least some bits of the time indicated by the time counter of the firewall.” Also, “the hash function comprises variables for a secret key, a source address, a source port number, a destination address, a destination port number, at least some partial bits of the ISN, a time indicated by the time counter of the firewall, which creates the m.SYN cookie, at the time of creation of the m.SYN cookie.”

In contrast, the blended SYN cookie disclosed by Fontes includes an index value and a hash value, in which the index value into a table of pre-configured sets of communications session parameters references one of the sets which approximates the desired communications parameters and the hash value is based on the source network address, a constant seed and current date and time data (See, e.g., lines 23-58, column 3; claim 1; and Fig.2.)

For an instance, since Fontes does not suggest or teach the time counter of the firewalls and cannot help but using regular current date and time data, the hash value in Fontes’s disclosure must be different in the structure and function. Fontes’s blended SYN cookie is distinctly different from the m.SYN cookie of the present invention.

In addition, the blended SYN cookie of Fontes is made with the SYN packet sequence number from the second stage, SYN/ACK packet, in TCP three-way handshake.

In contrast, in the present invention, the SYN packet sequence number of the SYN packet produced by the client in the first stage of the process is replaced with the m.SYN cookie. Also, a part of the SYN packet sequence number produced by the client is used to create the m.SYN cookie to support an incarnation of TCP connection, which is not suggested or taught by Fontes.

Fontes does not disclose the features of the present invention that the m.SYN cookie is used to communicate the information between the firewalls and share the status of the TCP connections across the firewalls.

As discussed above, neither Cheng nor Fontes teaches or suggests every elements and features of the amended Claims 1, 3, 4, and 6-10. Applicant respectfully submits that Claims 1, 3, 4, and 6-10 are patentable over Cheng or Fontes alone or in combination and request withdrawal of the rejections.

Dependent Claims

Although Applicant has not addressed all the issues of the dependent claims. Applicant respectfully submits that Applicant does not necessarily agree with the characterization and

assessments of the dependent claims made by the Examiner, and Applicant believes that each claim is patentable on its own merits. Claims 3, 4, and 6-10 are dependent either directly or indirectly on the above-discussed independent Claim 1. Applicant respectfully submits that pursuant to 35 U.S.C. § 112, ¶4, the dependent claims incorporate by reference all the limitations of the claim to which they refer and include their own patentable features, and are therefore in condition for allowance. Therefore, Applicant respectfully requests the withdrawal of all claim rejections and prompts allowance of the claims.

CONCLUSION

The Applicants have endeavored to address all of the Examiner's concerns as expressed in the outstanding Office Action. In view of Applicant's amendments to the claims and the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Should the Examiner have any remaining concerns, which might prevent the prompt allowance of the application, the Examiner is respectfully invited to contact the undersigned at the telephone number appearing below.

Respectfully submitted,

Date: November 2, 2007


James E. Bame
Regis. No. 44521
Tel: 213-384-7200
IPLA P.A.
3580 Wilshire Blvd 17th Fl.
Los Angeles, CA 90010